# Information Management & Security When Working From Home (Guidance)

The Law Society has provided downloadable templates and other material to assist legal practices to manage working from home.

This guidance should be used in addition to that material.

## Introduction

Working from home (WFH) increases the risks that:

- Correct information and documents are not available when required
- Unauthorised people gain access to client or practice information

## Risk considerations

Legal practices should consider the following risk factors:

- Information becomes dispersed across hard and digital formats and office and home locations
- Personnel access and update different versions of the same information, depending on where they work
- Personnel misplace hard format documents as they move to and from the office
- The home environment does not provide the same level of cyber and information security as the office
- Personal devices do not provide the same level of cyber security as work devices

## Control considerations:

To reduce these risks, legal practices should consider implementing the following control measures:

**Correct information and documents are not available when required**

- Agree and commit to maintaining a single source of truth for all information relating to all matters
  - » Ideally this will be a digital file, with processes to ensure all physical documents are scanned and placed in the digital repository
  - » Where this is not feasible, standardise the exceptions into a written procedure i.e. what hard documents must be kept in hard format and where are they stored for each file
- Review what hard format documents still arrive at the office (letters, court documents, etc.) and, based on who works at the office each day, document clear processes and responsibilities for opening, scanning, storing etc. in line with approach to single source of truth

## Unauthorised people gain access to client or practice information

- With your IT or cyber security advisor, review your current office-based cyber security measures and how these might be affected when people work from home and/or work from personal devices
- Consider applying the following policies, with exception by written approval
  - » personal computers shall not be used for work
  - » work computers shall not be used for personal matters
  - » no one other than practice personnel shall use work computers
- Provide technical support to personnel working from home to securely access the firm's IT systems via their home internet service, including where appropriate, assisting personnel with access to highly sensitive information or data to enhance the security of their internet router by:
  - » changing the router password
  - » updating its software
  - » disabling remote its access function
- Require of personnel working from home they:
  - » redo any previous cyber training (or provide training if this has not been previously offered)
  - » set auto-lock on work devices for a maximum of five minutes
  - » be conscious of who can see work at home
  - » ensure that videoconference or phone conversations cannot be overheard by other people at home
  - » use only designated videoconferencing platforms and control access via meeting password or administrator entry control
  - » be aware that videoconferences can be recorded
  - » do not use videoconference chat function to transmit sensitive information
  - » remove voice activated devices such as Alexa and Home from home offices